Privacy and Security Solutions for Interoperable Health Information Exchange

Final Assessment of Variations and Analysis of Solutions Report

Subcontract No.
RTI Project No. 9825

Prepared by:

William D. Hayes, PhD
Health Policy Institute of Ohio
37 W. Broad Street, Suite #350
Columbus, Ohio 43215

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

March 30, 2007

PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE
Final Assessment of Variation and Analysis of Solutions Report

Purpose of the Final Assessment of Variation and Analysis of Solutions Report

The purpose of the FINAL report is to refine and expand on the two previous interim reports.

This final report is a combination of the two interim reports and therefore does not ask that you think about the issues in different ways but rather provides the opportunity to expand on the earlier reports following the same format.

The only difference between this outline and the interim report outlines is the section numbering and changes needed to the introductory sections to combine the two reports and prevent repetition of sections.

The final report should clearly discuss the findings of the assessment of variation with regard to those variations *where privacy policy and security standards* are needed to preserve essential privacy and security protections and permit widespread interoperability.

Executive Summary

The purpose of the Final Assessment of Variations and Analysis of Solutions Report is to provide, for each state, a high-level summary of 1) variations discerned in the analysis 2) the status of current health information technology initiatives and 3) the most significant interim solutions proposed in their individual reports.

Adoption of HIT is on an upward trend in Ohio. The state created the Third Frontier initiative, a publicly funded effort to promote development and dissemination of cutting edge information technology across the state. Ohio is also working toward statewide coordination of HIE through public forums hosted by the Health Policy Institute of Ohio (HPIO), and through developing Regional Health Information Organizations across the state, two of which are currently actively engaged in health information exchange. HPIO has also coordinated the creation of an HIT/HIE Roadmap for Ohio with input from a broad stakeholder base, and is providing state legislators and the new governor's office with recommendations for moving forward with statewide coordination and monitoring of HIE efforts. Regional projects include:

- The Center for Healthy Communities (CHC) in Dayton has implemented an electronic shared, community-wide health record based on the Continuity of Care Record (CCR) standard

- HealthBridge in Cincinnati, an internet portal through which more than 100 entities supply, and thousands of users retrieve, laboratory reports in a standardized format
- The Community Health Alliance of Northwest Ohio in Toledo, an infrastructure that includes a neutral community-centric data processing center, and a highly leveraged service center
- Several Cleveland hospitals are working with one of the NHIN prototype demonstration projects to develop HIE architecture
- Cleveland Akron area NEORHIO, created in 2006
- In central Ohio, the major health systems and the business community, represented by some of the area's major employers, are working together to evaluate the feasibility of starting a local Community Health Network (CHN). The first phases of this evaluation will be focused on creating a self-sustaining business model centered on key initial deliverables provided by such a network, and finding appropriate funding sources for the formation of a RHIO to implement and support the CHN.
- The Appalachian Regional Informatics Consortium (ARIC) has been funded by the National Library of Medicine to create a sustainable and replicable model for advanced integrated information management systems for rural health care in Appalachian Ohio.

Ohio presented its solutions within six major groupings: 1) establishing national standards for HIE; 2) creation of a universal patient identifier (or method); 3) standardization of role-based system access models; 4) need for proactive financial support for the adoption of health IT; 5) need to address handling of sensitive health information; 6) need to focus the purpose of adoption of technology to improved quality of care. Recommended solutions included:

- Identify and use a unique identifier for patient identification, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included. In the future, accurate identification of patients should be through biometrics.
- Develop role based access standards and standard audit trails documenting by time and date stamp and source all read and write access to PHI.
- Standardization of the application of “medical need to know” and “minimum necessary.”
- States should take responsibility for developing the basic infrastructure to support health information exchange.
- Establish mechanism to allow electronic implementation of patient consent and adjust current laws and practices accordingly
- Adopt Continuity of Care Record (CCR) standard or other generally accepted standard for determining type of data routinely exchanged with regard to Medicaid, mental health, substance abuse and other diseases such as HIV/AIDS.

- Establish requirements that any publicly funded projects must conform to national standards including Continuity of Care Record (CCR).
- ERISA, FERPA and HIPAA regulations should be integrated.
- Consumer education is needed to articulate the perceived value of health information exchange against the perceived risk of privacy and security breaches in an electronic system.

1.0 Background and Purpose

1.1 Description of the purpose and scope of this report

The Final Assessment of Variation and Analysis of Solutions (AVARS) is to provide a consolidated view of the process and outcomes to the identification of variations, proposed solutions and the limitations inherent to the environment. This document is an extension of previous discoveries and further elucidation of continued investigations into legal barriers.

1.2 Description of level of HIT development in the state (e.g., beginning to advanced HIT development)

The Center for Healthy Communities (CHC) in Dayton has implemented an electronic shared, community-wide health record based on the Continuity of Care Record (CCR) standard. HealthBridge in Cincinnati, an internet portal through which more than 100 entities supply, and thousands of users retrieve laboratory test results in a standardized format. The Community Health Alliance of Northwest Ohio in Toledo is an infrastructure that includes a neutral community-centric data processing center, and a highly leveraged service center. Several Cleveland hospitals are working with one of the NHIN prototype demonstration projects to develop HIE architecture. Late in 2006, the Cleveland Akron area created NEORHIO. In central Ohio, the major health systems and the business community, represented by some of the area's major employers, are working together to evaluate the feasibility of starting a local Community Health Network (CHN). The first phases of this evaluation will be focused on creating a self-sustaining business model centered on key initial deliverables provided by such a network, and finding appropriate funding sources for the formation of a RHIO to implement and support the CHN. In the mostly rural southeastern part of the State, the Appalachian Regional Informatics Consortium (ARIC) has been funded by the National Library of Medicine to create a sustainable and replicable model for advanced integrated information management systems for rural health care in Appalachian Ohio.

1.3 Description of report limitations (e.g., scope limitations, process limitations, not all stakeholders included in project)

The groups that have participated in this process have determined that there are many solutions that can be addressed only by the federal government and those

solutions are not included in the scope of this report. It is critical to note that some federal solutions are prerequisite to any state based solutions.
To date the federal response to our assertions that standards are critical to assure interstate health information exchange has been met with a suggestion that states need to develop their own solutions to the lack of national standards. Our minority view that standards are in the federal domain will continue to be pressed by Ohio and shared with other states. Our primary concern is that in the absence of federal involvement multiple solutions will evolve that would not achieve interoperability.

Stakeholder participation was on the basis of who was available and able to attend or call into the meetings. There were some challenges of timing and scheduling in relation to community calendars and holidays. Recognizing that the staff and sub-contractors were the only paid participants, the number and persistence of the stakeholders represented is, we think, quite remarkable.

2.0 Assessment of Variation

2.1 Methodology Section

The Ohio Health Information Security and Privacy Collaboration (HISPC) project team employed a broad inclusive approach to collecting the information used in the completion of this report. The intent was to empower the stakeholders in the process and ensure a comprehensive response to the issues of privacy and security.

There were three work groups principally employed in the development of this report and the second project deliverable. The groups included the Variations Work Group (VWG), Legal Work Group (LWG), and the Ad-Hoc Work Group (AWG). Each group was comprised of members from a broad range of health care backgrounds thus assuring an expansive review of the issues. For example, the VWG membership included health care information technology consultants, chief information officers (CIOs), security officers, physicians, attorneys, health plans, hospital administrators, state health associations and state government representatives. In total, the VWG has 15 members to represent the stakeholder communities associated with this initiative. Similarly, the LWG is comprised of 29 members, of which 23 are attorneys and 2 are from other health care enterprises. Finally, the AWG consists of 46 members representing many stakeholder groups across the state of Ohio. The AWG was used throughout the project to supplement the information collection effort where representation on the VWG or LWG was lacking.

Each group conducted open meetings on a routinely scheduled basis. The method applied by the Ohio HISPC project team was to hold open discussions about health information exchange in the State of Ohio and surrounding states by

inviting participation of all interested parties and by targeting specific stakeholder groups for participation. A consensus model process that used nominal group process to explore objections and to articulate areas requiring more detail governs this “big tent” approach. This process provides the same type of consensus used by standards-developing organizations such as the American Society for Testing and Measurement. It streamlines discussion of the obvious, highlights distinctions and emphasizes the need to clearly articulate objections and nuances.

The process of information gathering required each group to first solicit input on the 18 scenarios from the group membership representing a particular stakeholder community. The VWG was the first to convene and review the scenarios. Initial feedback was provided to the LWG to ascertain if there were legal obstacles in Ohio that must be addressed before implementing any solution. The information was also provided to the AWG acting as an oversight committee and as supplemental staff to the VWG and LWG. Once the initial round of reviews was completed, the Ohio HISPC team, under the direction of William Hayes, President of HPIO, opened the dialogue to external stakeholders through a series of 20 Topical Area Meetings (TAMs). These meetings were open to the public and notice was posted on the project wiki site http://hispc.pbwiki.com . Specific stakeholder groups, such as pharmacy, long-term care, research, and rural health, provided the focus. Once the restriction for soliciting feedback from external stakeholders was lifted by the OMB, each participant in the Topical Area Meetings was asked to review the scenarios and post comments they might have through the wiki site. Those comments were forwarded to the VWG for a final review of the scenarios and the comments incorporated into this report.

Initial drafts of the report were provided to the work groups for comment. The *Interim Assessment of Variations Report* was then submitted to the project Steering Committee for final approval. Again, in the spirit of inclusiveness, each draft of the report was posted on the project wiki site with an invitation to external stakeholders to provide comment.

It is our opinion that broad-based consensus, one of the primary goals for the Ohio HISPC project, was achieved. Because all meetings were open and publicly advertised, dissent could be voiced at any point in the process. Electronic communication and teleconferencing technologies were used to assure broad geographical representation in all discussions.

2.2 Summary of relevant findings purposes for information exchange

2.3 **Treatment (Scenarios 1 - 4)**

2.3. a. *Stakeholders*

The principle stakeholders for the patient care scenarios include:

Hospitals, Physician Groups, Clinicians, Pharmacies and Behavioral Health

2.3. b. *Domains*

The primary domains associated with these scenarios include: User and Entity Authentication and Information Authorization and Access. The relevant business practices include *Request to Release Information* when the request is coming from an entity outside of the treatment facility; *Assessing Patient Competence* where the treating physician must determine if the patient is competent to authorize treatment or if a person with a durable power of attorney for health care is the appropriate decision-maker. In either case, federal and Ohio law provides that if a patient is confused to the point that she cannot give consent, an adult relative does not have status in Ohio to provide consent unless the adult relative is the patient's guardian or is the named durable power of attorney for health care. Additionally, HIPAA 45 CFR 164.510 may be a temporary solution/exception that would allow the daughter to assist with decisions about the mother's health care.

The barriers that exist in these scenarios relate to authenticating the requested PHI and a lack of national standards pertaining to the exchange of information. Our experience indicates that the electronic medical record is an aid to health information exchange but must be standardized among disparate systems to be fully effective.

Additional business practices of note include scenario #2's S*ubstance Abuse Physician Referral* that covers a referral from a substance abuse facility to a primary care physician. Due to the Federal Drug and Alcohol Confidentiality Act (42 CFR Part 2), if the client's authorization cannot be obtained, a Qualified Service Organization/Business Associate Agreement must be entered into between the treatment facility and the primary care provider prior to disclosure. The primary care provider could not disclose records received from the substance abuse treatment facility to a specialist without the patient's authorization due to 42 CFR Part 2 and Ohio law's prohibition on re-disclosure (42 CFR § 2.32, OAC 3793:2-1-06(H). Also, *Patient Consent* used to release Personal Health Information (PHI) to an external entity, S*pecialist Referral* should the primary care physician deem it necessary to seek the assistance of a specialist, *Provider Identification* used to validate the caregiver has appropriate authority to view patient information, *User Access* to ensure access is restricted to only those with a legitimate need to view the information based on specific roles, *Validation of Business Associate Agreements,* should such support organizations be included in the treatment protocol, *Record Update* to provide protocols when exchanging information with an external entity, and finally the *Universal Precaution* clinical business practice for emphasizing awareness of conditions requiring unusual

attention to prevent spread of infectious or contagious diseases. In that regard, the release of HIV information can only occur if the patient or patient's legal guardian specifically authorizes the disclosure of information to the requesting party in the written release (ORC 3701.243).

2.3. c. *Critical observations*

The reluctance to release (or re-release) PHI created by another entity is a pervasive problem based on a firm belief that it is prohibited. However, as long as HIPAA covered entities comply with privacy and security regulations, we are not aware of any legal basis for this position unless the Information to be released pertains to mental health issues, drug and alcohol issues or research protocols. Thus it is a barrier, but not a legal barrier. There is no legal obstacle to obtaining information from a prior treating hospital when an emergency room physician needs it for diagnosis and treatment. According to the scenarios, the previous treating hospital may be in a neighboring state so there would be sharing across the state line. HIPAA clearly allows this as part of the treatment exception and there is nothing in Ohio law that would prevent this request for information. The neighboring state may want a signed consent form to send the information.

As noted in scenario #3, the behavioral health unit would need to ensure its physical access controls satisfy the HIPAA physical safeguards requirements, which could also help the unit satisfy Ohio law. Additionally, there is a key consideration, regarding access to mental health information between the HIPAA requirements that apply on a national level, and provisions of the Ohio mental health law, which are stricter. The HIPAA standards only apply to covered entities (and their business associates), and the regulations do not preempt more stringent provisions of state law. See ORC 5122.31

Regarding release of other PHI information created by another care provider, this may be a barrier, but again not a legal barrier. HIPAA applies to protected health information that the covered entity creates or maintains as health information. We are not aware of a legal cite for saying that an institution should only produce the information that it creates, so there may be no liability issues. We do know that most physician offices and hospital stakeholders have an internal policy that states they will only give information that they create. If they obtain test results from another site (physician office or IDTF) they tell the patient to get the information from the original site. We are not aware that this is a legal requirement. We have only seen it as an institutional policy. In regards to scenario #2, it is important to note that the Federal Drug and Alcohol Confidentiality Act (42 CFR Part 2), which pertains to substance abuse patient records, covers virtually all substance abuse treatment facilities and is much stricter than the requirements of HIPAA.

2.4 **Payment (Scenario 5)**

2.4. a. *Stakeholders*

The principle stakeholders for payment scenario 5 include:
Payers, Consumers, State Government, Clinicians, and Hospitals

2.4. b. *Domains*

There are two primary domains identified for the payment scenario; Information Authorization and Access Controls, and Information Use and Disclosure. The first business practice identified by the stakeholders is *Payer User Access* for authenticating user need. Each stakeholder group has established differing procedures for authorizing access to patient information.

The methods used to satisfy this practice vary widely from telephone authorization to formal written request for access. Provided covered entities comply with existing statutes and regulations, this does not constitute a legal barrier. However, providing plan access through verbal authorization appears to have a high risk of unauthorized access based on a lack of documented authorization and may not satisfy the standard in 45 CFR 164.308. Health payers (other than workers' compensation) and health care providers are both covered entities as defined in CFR 45 106.103 and as such must comply with the minimum necessary standard set forth in 45 CFR 164.514(d). With regard to access levels, we have identified the *Minimum Necessary Information* business practice as critical to ensuring security and privacy of the electronic health record and further to provide that access is limited to the minimum necessary to satisfy the payers' needs. The flexibility of the minimum necessary standard itself creates interpretation challenges. This is an issue as it relates to privacy and security protocols.

2.4. c. *Critical observations*

The single most significant and recurring obstacle in all 18 scenarios is a lack of standardized procedures for sharing data. This appears to be true for all aspects of Scenario 5. However, provided the covered entities comply with existing regulations, this obstacle is not a legal barrier. Covered entities are required to implement security standards, including technical safeguards to ensure the confidentiality and integrity of PHI transmitted electronically under 45 CFR 164.312(e) (1). A provider and health plan would need to address the terms of the health plan's data access and limits thereof and agreement with the health plan. The transmission of data electronically would need to meet 45 CFR Part 162 requirements for transmitting electronic referral information (162.1301) and other standards as required, including the minimum necessary standard. An additional variable to consider in the payment scenario is workers' compensation, where the parties have rights of appeal on

treatment issues from a Managed Care Organization (MCO) to the Bureau of Workers' Compensation and to the Industrial Commission [See OAC 4123-6-16; ORC 4123.511]. Limiting access to records the MCO reviewed in making its initial determination may pose due process problems, since Ohio WC is a governmental function. In addition the VWG and LWG identified the following observations relevant to scenario 5. Authorization is required under HIPAA for psychotherapy notes 45 CFR 514(d)(2). Ohio law prohibits disclosure of HIV status without authorization (ORC 3701.243). State workers compensation statute governs disclosure for WC benefits 45CFR 512(l); O.A.C §4123-6-20(D).

2.5. **RHIO (Scenario 6)**

2.5. a. *Stakeholders*

Regional Health Information Organizations, RHIOs, physicians, consumers and other health care providers.

2.5. b. *Domains*

The primary domain for this scenario is Information Use and Disclosure policies. *Role Based Access,* defining who has access to information at a specific level is the principle business practice. The disease management issue described in this scenario, while not specifically stated as such, could have research ramifications and falls into the same area as the *Research Request* business practice identified in Scenario 7. The monitoring of each provider in the manner of treatment is a quality review practice that is typically done by healthcare payers not RHIOs. This scenario does not specifically state the data is required for research purposes. If the use is for research purposes, the RHIO board would provide a mechanism for review of all report requests and would follow IRB protocols with respect to aggregate data and reports.

2.5. c. *Critical observations*

A RHIO is a neutral trusted third party intended to facilitate effective health information exchange to improve the quality of patient care by providing comprehensive information at the point of care. Each RHIO board will have to establish business rules about the types of data usage that will be permitted. It is interesting to note that two of the Ohio RHIOs (Dayton and Athens) are administratively housed in Schools of Medicine with already established business rules, Internal Board of Reviews and other institutional supports. Some RHIOs provide reports back to user organizations to facilitate and encourage self monitoring. However information, like that described in the ranking of providers, would likely jeopardize the neutrality of the RHIO. Existing Ohio RHIOs use aggregated information in community health planning; for example responding to the needs of the uninsured and underinsured, health risk factors, etc. In this scenario, the fulfillment of the first item is, "The RHIO in your region wants to access patient identifiable data from all participating

organizations (and their patients) to monitor the incidence and management of diabetic patients." There is no reason to maintain patient identifiable data to assess the management of diabetic patients as a class. In current practice, Ohio RHIOs would only use aggregate or de-identified information to evaluate treatment or outcomes. Trends are analyzed for public health and other planning purposes. Recognizing that disease management is a complex process that includes the patient, environment, health care providers and health educators, the only effective response must focus on all of those systems, not target only one. The second item in the scenario description "… the RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients," is unlikely to occur in existing RHIOs given the need for neutrality and interest in promoting broad participation. The only way this might work would be to provide information confidentially to practices and providers. This would provide a self-evaluation process with data for each practice benchmarked against a set of community level data. The underlying difficulty with this scenario is that it assumes that health information exchange will be limited to existing paradigms, ones that look at diseases, transactions and "bits" of health information. This bifurcated view of health and health care does not support the new paradigm of patient centric health care. A holistic view of patients in the practice of medicine is necessary to integrate health knowledge management into the practice of medicine.

Because the RHIO is not a covered entity or an organized health care arrangement, patient authorization meeting HIPAA requirements would be required for a participant organization disclosure to the RHIO unless the information is used and disclosed pursuant to a HIPAA compliant business associate agreement. If no BA agreement is in place, patient authorization to use and disclose would be a significant barrier 45 CFR 164.502(e), 45 CFR164.508.

Research (Scenario 7)

2.6. a. *Stakeholders*

The primary stakeholders include: Hospitals, Clinicians, Consumers, Laboratories, Government Payers and Research Sponsors, Private Payers, and Other Corporate Research Sponsors.

2.6. b*. Domains*

The primary domain identified for this scenario is Information Use and Disclosure Policy. There are two principle business practices to consider. The *Research Request* business practice asserts that all research projects fall under the auspices of the Institution Review Board (IRB). *Deviation of Intent* addresses the practices followed should variations arise to the original intent of the research project. Should the need for variations arise, the practice requires re-submittal to the IRB for additional approval. The

Common Rule, 45 CFR 46.103(b) requires that an IRB review and approve research involving the use of human subjects or individually identifiable health information. In addition to the Privacy Rule's individual authorization requirement, the Common Rule requires that a signed consent be obtained from potential research subjects, which explains the potential benefits and risks associated with their participation in the study.

2.6. c. *Critical observations*

The Health Insurance Portability and Accountability Act (HIPAA) Standards for the Privacy of Individually Identifiable Health Information (the Privacy Rule) require that a prospective research subject execute a written authorization to allow an investigator to use a subject's individually identifiable health information for research purposes, including incorporating the information into an electronic database for the study. In the case of minors, a parent or legal guardian must complete the HIPAA authorization on the child's behalf. The authorization must describe, with specificity, what the health information will be used for, who will have access to the information (including, for example, the principal, the co-investigator, the institutional review board (IRB) reviewing the research, the sponsor, and federal oversight agencies such as the Food and Drug Administration), how long the information will be used, and that the subject's health information will be placed in a database for the project.

The HIPAA Privacy Rule requires that an authorization describe to subjects who will have access to their individual health information used in the study, as well as how long the information will be kept or used. Similarly, the Common Rule requires the IRB to approve the study methodology, including how the database will be accessed, used and secured. Both the Privacy and Common Rules, however, provide mechanisms that allow the use of study data by researchers not included in the original IRB-approved protocol and disclosed to subjects in the HIPAA authorization. Specifically, both the Privacy Rule and guidance from the federal Office of Human Research Protections allow the research data to be de-identified and provided to the postdoctoral fellow for use in a white paper not related to the original research. In order to provide individually identifiable health information to the fellow, however, the principal investigator must obtain re-consent and authorization from the subjects for use not included in the original protocol and authorization. The Rules also provide a mechanism for the investigator and fellow to formally request a waiver of individual authorization and informed consent from the IRB - if specific criteria including the Rules are met.

The federal Food and Drug Administration (FDA) Policy for the Protection of Human Subjects, however, does not generally allow waivers of informed consent. As a result, the white paper could not be used to support a new drug application submitted to the FDA.

If an investigator wants to extend the length of the study to collect and track personal health information beyond the time frame specified in the consent and authorization and approved by the IRB, the Privacy Rule and the Common Rules requires that subjects consent to the proposed additional use. As noted previously, both the Privacy Rule and Common Rule, however, allow the principal investigator to request a waiver of individual authorization and consent from subjects if the specific criteria in the Common Rule are met. Such criteria include the practicability of obtaining re-consent as well as the nature and risks and benefits associated with the proposed additional use. In this scenario, however, a waiver is unavailable, since the research involves the study of a new ADD/ADHD drug, which is regulated by the FDA. As a result, the principal and/or co-investigator will likely need to again obtain consent from the subjects and their parents or guardians in order to collect individual health information for an additional six- month period. 45 CFR 46.101, 21, CFR 50.20, 21, CFR 50.23, 45 CFR 164.512, and Department of Health and Human Services Office for Human Research Protections August 10, 2004 Guidance on Research Involving Coded Private Information or Biological Specimens

2.7 **Law Enforcement (Scenario 8)**

2.7. a. *Stakeholders*

The primary stakeholders include: Hospitals, Clinicians, Consumers, Laboratories, Payers and Government

2.7. b. *Domains*

There are two primary domains, Information Use and Disclosure and State Law that are applicable to this scenario. Three business practices have been identified for this scenario. The first, *Request by Law Enforcement* addresses the need to validate a request from law enforcement to release patient information without a client authorization. To release the patient's blood alcohol test results to the police officer pursuant to HIPAA 45 CFR 164.512(f)(1), the disclosure would have to be required by state law, or pursuant to: a court order or subpoena or summons issued by a judicial officer, grand jury request, or an administrative request (administrative subpoena, summons, authorized investigative demand) that is relevant and material to a legitimate law enforcement inquiry, specific and limited in scope and not able to be provided in a de-identified format. To be a required disclosure under state law (ORC 2317.022), the officer would have to submit a "written statement requesting the release of records" indicating that an official criminal investigation has begun regarding a person, pursuant to Ohio law. The second business practice, *Request from Law Enforcement,* pertains to law enforcement access being limited to specific electronic records that are the subject of the request because it is not authorized to view entire medical record. The third business practice identified by the work groups is *Authorization Review.* Pursuant to HIPAA, the parents of an adult child are not permitted to review the Emergency

Room record and laboratory results unless the patient signs an authorization allowing for the disclosure OR the parents have been designated by the son as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions per 45 CFR 164.502(g)(2).

2.7. c. *Critical observations*

Parents of an adult child are not permitted to review the Emergency Room record and laboratory results of that child unless the patient signs an authorization allowing for the disclosure 164.508(a) OR the parents have been designated by the child as an "attorney in fact" in a durable power of attorney for health care and the child was not competent to make his own health care decisions per 45 CFR 164.502(g)(2). In addition, the parent's receipt of Explanation of Benefits from their insurance company often contains enough descriptive information about billing for the health care service to enable parents to learn medical information to which they would not otherwise be entitled. This situation can be a barrier to care if a person decides to forego care because a related or unrelated third party is responsible for payment. One final note, the Federal Drug and Alcohol Confidentiality Act does not apply to most general emergency room visits 42 CFR 2.12(e)(1).

2.8 **Prescription Drug Use/Benefit (Scenarios 9 and 10)**

2.8. a. *Stakeholders*

The primary stakeholders for scenarios 9 and 10 include: Clinicians, Payers, Clinics, Consumers, Pharmacy, and Behavioral Health organizations

2.8. b. *Domains*

The domains identified for these scenarios are Information Use and Disclosure and User and Entity Authentication. There are several business practices that were identified as applicable to both scenarios. The first business practice *Patient Authorization and Verification of Access* addresses the requirement to obtain permission from the patient to share information with an appropriate business entity. There must be a process to validate appropriate use by an entity prior to accessing a specific class of patient data. The patient authorization to release information must be specific and based on needs of the sharing entities. The second business practice is a repeat of the need to create an appropriate *Business Associate Agreement.* The agreement is required to permit sharing of information between the hospital/provider entity and the Pharmacy Benefits Manager (PBM). Consistent with the BAA is the business practice to provide *Minimum Necessary Release of Information that* is a HIPAA requirement under 45 CFR 164.502.

2.8. c. *Critical observations*

In reviewing theses scenarios the work groups expressed several concerns. First, they expressed concern over the method for exchanging and receiving the request for information. Members of our stakeholder

community suggested a telephone call with call back procedure was sufficient to satisfy user authentication. Others suggested the request should be made by fax. To that end, ORC 4729.37 and OAC 4729-5 contemplate phone and fax contacts and set forth the procedure and record keeping requirements. 45 CFR 164.312 requires reasonable measures to safeguard electronic transmission of PHI. Secondly, they noted that the procedures may result in a delay to treat the patient. In addressing this concern, 42 CFR 423.566, .568, .570 and .578 requires timely benefit determinations, expedited coverage decisions and exceptions. Thirdly, they noted concern regarding the potential for the PBM to be outside the patient area of residence. In such a case, if the PBM has entered into a contract with an Ohio employer to provide services to Ohio residents, to the extent applicable, the PBM would be subject to Ohio law. The hospital as a self-insured employer is subject to ERISA requirements concerning the proper administration of its health plan. The PBM as a subcontractor of hospital should be required to follow the same ERISA rules.

2.9 **Healthcare operations/marketing (Scenarios 11 and 12)**

2.9. a. *Stakeholders*

The primary stakeholders in scenarios 11 and 12 are consumers, hospitals, and clinicians.

2.9. b. *Domains*

The principle domain is Information Use and Disclosure and there are two principle business practices of note. *Request for Review* provides the Privacy officer will review all requests for information from the Marketing Department. The concern is for the level of consent required to satisfy the request. This depends on the nature of the integrated health delivery system. If ABC Health Care itself is a HIPAA "covered entity" (as opposed to holding company or corporate entity that does not provide covered services), it (along with its affiliated hospitals) could be part of an organized health care arrangement (OHCA) or an affiliated covered entity (ACE) under HIPAA. In such case, the use and disclosure of Personal Health Information (PHI) by ABC (as part of the OHCA or ACE) would be the same as use and disclosure of the affiliated hospitals. If ABC Health Care is not a covered entity, the communication activities must emanate from the hospital (i.e., covered entity) level. The first consideration is whether the critical access hospital can disclose PHI to DEF Medical Center for it's "health care operations" under 45 CFR 164.506(c)(4). If the covered entities cannot share/disclose PHI, each of the hospitals must make the communications with its own patients.

The definition of "marketing" under HIPAA is the key to the analysis of whether these communications are permissible under HIPAA. Under 45 CFR 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the

covered entity making the communication,...or (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual." Thus, it would appear that DEF could make the communication with all patients (assuming it properly received the PHI as part of an OHCA, ACE or for health care operations) under clause (i) above -- or each of the affiliated critical access hospitals could make the communication as a recommendation of "alternative health care providers or settings of care" under clause (iii) above. The second, and perhaps more significant business practice, involves securing the *Patient Authorization.* Our stakeholders suggest it is the Marketing Department that has primary responsibility for securing the patients' release to use their information pursuant to CFR 45 164.508.

2.9. c. *Critical observations*

Patient authorization is not needed for the hospital to send information to its patients concerning the services available at the hospital. See 45 CFR 164.501 (definition of "marketing"). Providing patients with information on the hospital's new pediatric wing/services is a permissible purpose and is not considered "marketing" for HIPAA purposes. Under 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the covered entity making the communication." Based on OCR guidance, it appears that these communications can be targeted to patients of the hospital who recently gave birth. The Privacy Office and Marketing Departments must determine what mode of transferring information will be used and the type of information, i.e., identifiable or de-identified information will be provided to the marketing department. Resolution of this issue will depend on the facts, which should be analyzed on a case-by-case basis, but the activities described can be undertaken without de-identifying the PHI if all applicable HIPAA requirements are met (e.g., the minimum necessary standard). Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).

Additional concerns were raised regarding the disclosure of health information of Medicaid recipients. Even in that regard there was not unanimous consensus on how the rules are applied. Proponents of the application of the rules in the scenario noted that essentially, the 42 CFR 431 Subpart F (Entitled Safeguarding Information on Applicants and Recipients) restricts disclosure of information to "purposes directly connected with the administration of the plan." Those are defined as establishing eligibility, determining the amount of assistance, providing services for the recipients (within the plan — which means the state plan, or the state's Medicaid program), and assisting or conducting investigations, prosecution of civil or criminal proceedings related to the administration of the program (42 CFR 431.302). The subpart requires that the Ohio Department of Jobs and Family Services (ODJFS) have

restrictions in place and that the restrictions apply to those to whom the information is released that require them to be under the same standards of confidentiality as the agency itself. Thus, the hospital is under the same standards of release of the information as ODJFS (42 CFR 431.306). The types of information subject to the safeguards includes names and addresses, medical services, social and economic conditions, evaluations of personal information, medical data (including diagnosis and past medical history), information received for verifying income eligibility, and any information regarding identity of third party resources (42 CFR 431.305). There is also a requirement similar to the HIPAA requirement that only the minimum necessary information be released if the conditions are met for such release. Ohio Revised Code Section 5101.27 covers not only Medicaid but all public assistance programs and restricts the release of information to the recipient, an authorized representative, legal guardian, or the attorney of the recipient (but only if there is written authorization that complies with ORC 5101.271). ORC 5101.27(D) permits the release of information if the recipient provides voluntary, written authorization and the release is permitted by federal law. ORC 5101.27(F) permits the release by the agency (and by extension, and through the provision in the provider agreement that subjects a provider, including a hospital, to the same confidentiality restrictions of the agency) if the release is for purposes "directly connected to the administration of or provision of medical assistance provided under a public assistance program" and the information is released to an entity subject to the standards of confidentiality comparable to those of the agency.

An alternative viewpoint on the 42 CFR 431 Subpart F issue is that it does not specifically apply to health care providers. Rather, it is federal law imposing requirements on state Medicaid agencies. It requires a state Medicaid agency to adopt rules to govern its own practices to ensure that it safeguards the information of its applicants/recipients. The law cited as authority for binding providers to the state Medicaid agency standards (42 CFR 431.306) provides in the pertinent subsection (b): “Access to information concerning applicants or recipients must be restricted to persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the agency.” In the absence of specific law governing healthcare providers, this provision does not appear to provide definitive authority for the proposition that all healthcare providers must adopt separate policies for the use and disclosure of the protected health information of Medicaid applicants and recipients.

2.10 **Public Health/Bioterrorism (Scenario 13)**

2.10. a. *Stakeholders*

The primary stakeholders are clinicians, Physician Groups, Federal Health Facilities, Hospitals, Payers, Public Health, Community Clinics, Lab,

Pharmacies, LTC, Hospice, Correctional Facilities, State Government, Trauma Centers and Poison Control Centers.

2.10. b. *Domains*

The primary domain for this scenario is State Law Restrictions. The business practice identified is *Reporting a Bioterrorism Event.* This practice involves an entity making a telephone call notification of a possible event followed by fax verification to state authorities. Boards of health, health authorities or officials, health care providers in localities in which there are no health authorities or officials, and coroners or medical examiners shall report promptly to the department of health the existence of any of the diseases or illnesses listed in Ohio Administrative Code 3701-3-02. The individually identifiable health information reported to public health agencies is protected (confidential and not subject to disclosure) pursuant to R.C. 3701.17. Additionally, pharmacies, poison control centers, and other health-related entities are required to inform public health agencies of unusual events per R.C. 3701.232 and 3701.201. However, during an actual terrorism event, the Federal Bureau of Investigations will be the lead agency, under Presidential Decision Directives 39 (1995) and 62 (1998); see, 10 USC 382, 18 USC 175-178, 18 USC 2331-2339B. Communication and the transfer of data outside public health or hospitals will occur on an "as needed" basis and will be conducted primarily via telephone and secure facsimile transmissions. In that regard, timing of required communications are governed by Ohio Administrative Code 3701-3-05 and 3701- 3-06. Additionally, HIPAA requires an accounting of the disclosures and procedures. See 45 CFR 164.528.

2.10. c. *Critical observations*

The means and timing of communicating information on reportable disease cases is set forth in Ohio Administrative Code 3701-3-05 and 3701-3-08. In Ohio it is generally believed that all entities are aware of the State reporting procedures and can find additional information at"

"Know your ABCs" – **http://www.odh.ohio.gov/pdf/idcm/intro9.pdf**;

"Infectious Disease Control Manual" - **http://www.odh.ohio.gov/healthresources/infectiousdiseasemanual.aspx.**

There are no legal barriers preventing the exchange of information in this scenario, however, an attitudinal barrier exits. Some providers refuse to comply with state reporting requirements.

2.11 **Employee Health (Scenario 14)**

2.11. a. *Stakeholders*

Hospital, Payer, Consumer, Payer and Clinician

2.11. b. *Domains*

There is one domain associated with this scenario, *Information Authorization and Access Control* and two primary business practices. The first practice is *Authorization to Release Information* and involves

obtaining patient authorization to release information for purposes other than treatment, payment or health care operations (TPO). HIPAA-compliant patient authorization is required for this non-TPO purpose, which should be easily obtained because the disclosure is for the patient's benefit **(**See 45 CFR 164.508). If a hospital has patient authorization there is no barrier to electronically generating a return to work document to be given to a patient or to an employer or other party per the patient's authorization.

The second business practice is the *Data Transmission Protocol* and involves physician verification that the patient can return to work. The stakeholders in the work groups suggested this is currently accomplished through both voice and fax communications. The preference is to transmit over secure e-mail to a secure fax receiver. With respect to restrictions related to minimum necessary the terms of the authorization establish the limits of the PHI that can be disclosed. The minimum necessary standard does not apply to disclosures made pursuant to an authorization (See 45 CFR 164.502(b)(2)(iii).

2.11. c. *Critical observations*

A cut and paste approach referenced in the scenarios does not pose legal problems, provided that the PHI that is cut and pasted meets the requirements of the authorization. A possible exception to this is that the covered entity must ensure that metadata or hidden text is not transferred during the cut and paste process. A practical problem may exist because it would seem more likely that PHI beyond the scope of the authorization could be inadvertently included in the disclosure if a cut and paste process is used. Members of our work group noted that problems that arise in this area are often due to follow-up calls from employers that seek additional information regarding the employee/patient. Providers (and their staff) need to ensure that all PHI disclosed during follow-up conversations/disclosures is within the scope of the authorization allowing the initial release of the PHI.

2.12 **Public Health (Scenarios 15 – 17)**

2.12. a. *Stakeholders*

Public Health, State Government, Consumer, Law Enforcement, Clinicians, Hospital, Laboratory, Behavior Health, Community Clinics and Health
Centers, Medical and Public Health Schools and Public Health Agencies

2.12. b. Domains

The primary domains for scenarios 15-18 include: State Law Restrictions, Information Authorization and Access Controls, and Information Transmission Security or Exchange Protocols. There are a number of business practices including *Exchange of Health Information* which identifies the processes for exchanging information among multiple

entities within the State; *Mandatory State Requirements* that defines State requirements for reporting mandated screening tests for infectious disease; *Minimum Necessary Guidelines* as discussed previously in this report; *Authorization to Treat* and the requirement to obtain authorization from a patient prior to treatment protocol; *Alternate Authorization* that addresses the requirement for a BAA in the absence of patient authorization; and *State Reporting* outlines the protocols for mandatory reporting.

Under Ohio statutes and regulations, medical providers and laboratories are required to report diagnoses or laboratory results that identify a communicable disease listed in state regulations to local and state health officials. These diseases are considered by public health officials to represent a danger to public health. RC 3701.23 and OAC 3701-3-01 et seq.; see R.C. 339.78. The director of the Ohio Department of Health (ODH) has statutory discretion to share information necessary to "control, prevent or mitigate disease." RC 3701.14(J); see RC 3701.17 and 339.81. ODH works with other state health departments and the Centers for Disease Control and Prevention, with the latter's authority at 42 USC 264 et seq. and 42 CFR Parts 70 and 71. Federal and state statutes and regulations enable governmental response to communicable, infectious diseases to be appropriate to the size of the risk. There are no obstacles other than risk for inappropriate response by public or private parties. Substantial state and federal legal authority exists that enable state and local health departments to screen for communicable disease, mandate treatment, provide for isolation or quarantine, share PHI with persons or entities necessary to control, prevent or mitigate disease, and utilize law enforcement to enforce. Such authority enables government to screen and manage such situations irrespective of a patient's mental health.

Regarding scenario 16, Ohio does not use an Interactive Voice Response System for newborn screening because it cannot verify the caller (the person or entity). As the official testing laboratory for Ohio, ODH receives actual blood spots from providers and then faxes results of screenings to the submitting providers. To ensure accurate communication and given the insecurity of email, ODH maintains a self-identified facsimile number for every provider. ODH puts responsibility for security of faxed information on the provider receiving the fax. The only alternative would be for each provider to own a mass spectrometer (the device needed for the testing) and ODH would only function as a results repository – could only have a completely electronic exchange of samples and results if every provider had the machine - defeats purpose of state lab doing the testing. Also, Ohio only performs limited tracking subsequent to newborn screening. Confidential newborn screening results are sent to the birth hospital and to the physician of record.

With respect to Scenario 17, the shelter is not a covered entity under HIPAA and could therefore share information with the relative. The drug program could not share any information with the relative without an authorization pursuant to the Federal Drug and Alcohol Confidentiality Law (42 CFR § 2.33) and OAC 3793:2- 1-06(H). The primary care physician could share information with the relative if the patient signs an authorization allowing for the disclosure OR the relative has been designated by the patient as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions. The drug clinic would need a client authorization or a Business Associate Agreement/Qualified Services Organization agreement with the county to share information with the county for the purposes of program reimbursement pursuant to the Federal Drug and Alcohol Confidentiality Law and Ohio law.

2.12. c. Critical observations

Several issues arise from this collection of scenarios that the VWG and LWG chose to address. With respect to scenario B and newborn screening and whether or not newborn screening data can be transmitted electronically the groups found the newborn screening statute renders the information confidential. Results are sent to the birth hospital and to the physician of record (POR). The Ohio Department of Health security policies and procedures are stricter than the HIPAA security rule standards because of terrorism issues. No state law mandates a tracking disclosure of PHI or authorizes a public health authority (Ohio Department of Health) to track the child over time. This is a potential privacy concern barrier because no law governs should the state wish to conduct tracking over time. ODH does some follow-up to make sure the child is referred to a care provider but management of care is left to care providers. See ORC 3701.501 et al., OAC chapters 3701-55 and 3701-36, and 45 CFR 164.512 (a) and (b).

With respect to Public Health Scenario C the VWG and LWG identified that the shelter is not a covered entity and could share its information with the relative. The drug program could not share any info without an authorization 42 CFR § 2.33, OAC 3793:2-1-06(H). The primary care physician (PCP) could share information with the relative if the patient signs an authorization allowing for the disclosure 164.508(a) OR the relative has been designated by the patient as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions. Also based upon the facts presented, there may be an additional potential legal obstacle in scenario 17. The facts presented do not indicate whether the homeless man receives public assistance. The fact that the man has a primary provider and the statement that the man is to be sent to a hospital-affiliated drug treatment facility "for his addiction under a county program" lends credence that the homeless man may be receiving public assistance, which may include a

public medical assistance program or Medicaid coverage for medical assistance. If the homeless man does receive a medical benefit through a public medical assistance program the confidentiality statutes may restrict the release of information. ORC 5101.27 addresses all public assistance, including Medicaid. If the homeless man receives, or is eligible for, Medicaid, confidentiality of information is also subject to 42 CFR 431 Subpart F and OAC 5101:1-37-01.1.

2.13 **State Government oversight (Scenario 18)**

2.13. a. *Stakeholders*

Public Health, State Government, Consumer, Law Enforcement, Clinicians, Hospital, Laboratory, Behavior Health, Community Clinics and Health Centers, Medical and Public Health Schools and Public Health Agencies

2.13. b. *Domains*

The primary domains for scenario 18 include: State Law Restrictions, Information Authorization and Access Controls, and Information Transmission Security or Exchange Protocols. There are a number of business practices including *Exchange of Health Information* which identifies the processes for exchanging information among multiple entities within the State; *Mandatory State Requirements* that defines State requirements for reporting mandated screening tests for infectious disease; *Minimum Necessary Guidelines* as discussed previously in this report; *Authorization to Treat* and the requirement to obtain authorization from a patient prior to treatment protocol; *Alternate Authorization* that addresses the requirement for a BAA in the absence of patient authorization; and *State Reporting* outlines the protocols for mandatory reporting.

Under Ohio statutes and regulations, medical providers and laboratories are required to report diagnoses or laboratory results that identify a communicable disease listed in state regulations to local and state health officials. These diseases are considered by public health officials to represent a danger to public health. RC 3701.23 and OAC 3701-3-01 et seq.; see R.C. 339.78. The director of the Ohio Department of Health (ODH) has statutory discretion to share information necessary to "control, prevent or mitigate disease." RC 3701.14(J); see RC 3701.17 and 339.81. ODH works with other state health departments and the Centers for Disease Control and Prevention, with the latter's authority at 42 USC 264 et seq. and 42 CFR Parts 70 and 71. Federal and state statutes and regulations enable governmental response to communicable, infectious diseases to be appropriate to the size of the risk. There are no obstacles other than risk for inappropriate response by public or private parties. Substantial state and federal legal authority exists that enable state and local health departments to screen for communicable disease, mandate treatment, provide for isolation or quarantine, share PHI with persons or

entities necessary to control, prevent or mitigate disease, and utilize law enforcement to enforce. Such authority enables government to screen and manage such situations irrespective of a patient's mental health.

2.13. c. *Critical observations*

Regarding Scenario 18, Health Oversight, the VWG and LWG noted significant barriers with respect to most aspects of the contemplated information exchange: 1) there are few, if any, common formats and identifiers in order to allow for meaningful exchange of information among agencies and between several states which affects tracking processes; 2) there are barriers imposed by requirements for business associate agreements, data use agreements or governmental memoranda of understanding; 3) Medicaid regulations may preclude the disclosure of some of the information; 4) the Family Educational Rights and Privacy Act (FERPA); 34 CFR Part 99, applies to educational records and may be implicated by this scenario – the privacy protections under FERPA are not entirely consistent with HIPAA, authorization/consent will likely be required by parents for the release of the educational record, though there is an exception that may or may not apply to this scenario (34 CFR 99.31 permitted disclosures in cases of health and safety emergency). Additional regulations that may apply include: 42 CFR Part 431 Subpart F Safeguarding Information on Medicaid Applicants; state laws and regulations restricting the release of information regarding recipients of public assistance programs including Medicaid; ORC Section 5101.27 and OAC Section 5101:1-37-01.1; and HIPAA restrictions and requirements for uses and disclosures of protected health information at 45 CFR 164.502, 164.504, 164.508, 164.512, and 164.528

2.14 Summary of Critical observations and key issues

- *Introduction to the section*

Over the course of this project the Variations Working Group and Legal Working Group were able to identify a number of key issues that impact the HISPC efforts. They include the following:

- The single largest obstacle to open information exchange and interoperability is a lack of credible data standards shared by all stakeholder entities. Numerous efforts have been made including the HL7 initiative; however, resistance from the software development industry has kept this issue unresolved. Until standards for data exchange, including consistent data formatting and exchange protocols are adopted, this issue will remain unresolved, and the opportunity to enact true systems integration will remain unfulfilled.
- There are relatively few legal obstacles preventing the exchange of electronic health information. Adoption of the HIPAA guidelines has provided the individual states an opportunity to develop internal standards for patient privacy and security. In many cases the state standard exceeds

that mandated at the federal level providing a higher expectation for securing the health record. This does create some differing standards, however, that must be reconciled in practice.

- There is widespread consensus that the patient electronic health record can contribute to improved management of ones individual health. The challenge is to develop systems that are affordable to all levels of the health care delivery system. Adoption of this tool is occurring in the larger delivery systems supporting an urban community. However, adoption in the rural areas has lagged behind the urban communities principally as a result of limited funding.
- Lack of a standardized patient identifier is inhibiting electronic exchange of information. Disparate systems with identifiers unique to the individual systems have limited interoperability, creating inefficient interfaces, and jeopardizing the integrity of the data exchange.
- Universally, the physician members of the work groups suggested that treatment of the patient is the first priority in an emergency and obtaining consent or other administrative task is not a primary consideration.
- As a general rule the groups agreed there is a need for a consistent method to authenticate a user request. This can be easily accomplished through the use of fax technology or through more sophisticated use of network devices using standardized login protocols.
- Use of the HPIO wiki site proved to be a valuable tool for the dissemination and collection of data and for providing information to the general community at-large.
- Ohio law requirements that are applicable to mental health records and stricter than HIPAA, and the very restrictive requirements of the Federal Drug and Alcohol Confidentiality law that are applicable to alcohol and drug abuse patient records, pose an additional challenge to the exchange of health information.
- Effective, statewide and national health information exchange will only be successful when there is a major commitment from the state and federal government to find mechanisms for funding the necessary initiatives that will enable exchange. In Ohio we observe that no single health care sector is positioned or able to provide the necessary funding to jump start health IT or exchange of information. There does not appear to be sufficient collective will in the private sector to fund health information exchange outside of localized efforts where return on investment can be quantified. Even then, some sectors cannot afford the investment that is necessary. The private sector is not likely to step up to the plate unless there is significant public sector financial support to fund well articulated policy objectives.

3.0 Summary of Key Findings from the Assessment of Variation

- Description of the main findings from the Interim Assessment of Variations Report, prioritize key findings (top 5 to 10 identified privacy and security issues), and the rationale for prioritization.

Several significant findings were identified by VWG that must be addressed for this initiative to succeed. These findings include:

Barrier 1: Establishing national standards for data exchange that must be adopted by all parties involved in the exchange of patient health information (PHI). The lack of any such standards coupled with the absence of an enforcement agency is the primary reasons for the failure to gain system interoperability across health care entities.

Barrier 2: Creation of a universal patient identifier (or method) will also be a valuable tool in assisting data exchange and improving the security and privacy of the patient information.

Barrier 3: It is our recommendation that the use of a role based system access model be standardized and implemented across the full spectrum of health care entities.

Barrier 4: Funding, especially for rural communities, is a significant barrier to adoption of standards. As such, it is critical to have proactive financial support by the state government and/or through the development of public and private partnerships in Ohio. To that end, it will be most important for all stakeholders to be actively engaged in this effort.

Barrier 5: Federal and state law requirements applicable to mental health, Medicaid, HIV/AIDS, and substance abuse records are stricter than the requirements of HIPAA.

Barrier 6: The use of technology is viewed as a tool to improve systems interoperability with respect to privacy and security of information; however, it should not be implemented in the absence of a firm commitment to improving quality of care.

- Description of ‘effective’ practices identified by the state, including overall practices that protect privacy and security and permit or advance interoperable electronic health information exchange (and that cut across multiple domains specified in the contract) as well as practices identified within each of the nine domains (a brief description of the definition of ‘effective’ practice should be provided)

Effective practices that we have identified include (1) locally initiated development of RHIOS around the state, (2) annual and special purpose meetings that convene stakeholders are a part of ongoing Ohio picture, (3)

hospital based quality initiatives and (4) initiatives in state offices that have begun to address best security practices.

Establishing locally initiated RHIOs around the State's major population centers administered by neutral and trusted third parties is pivotal to secure exchange of information and identified as an effective practice. The two RHIOs currently exchanging data use standard HIPAA procedures (Business Associate Agreements and Data sharing agreements) to establish privacy and security parameters and responsibility. The two RHIOs that exchange electronic information are HealthBridge in Cincinnati (the result of a successful CHIN effort) and HealthLink RHIO in Dayton, (the result of a HRSA HCAP grant). HealthBridge has a business model that requires demonstration of return on investment prior to developing additional functionalities, assuring sustainability. HealthBridge provides a portal and delivers lab results to providers. HealthLink RHIO in Dayton uses an Application Service Provider (ASP) model for sustainability using subscriptions to support a public utility model for health information exchange. HealthLink RHIO with its HIEx™ application and data base is using the UMLS (Unified Medical Language System) from the National Library of Medicine (NLM) as the data for tables specified in the Continuity of Care Record. To date HIEx™ offers Medications, Diagnoses, Immunizations and Procedures.

HealthLink RHIO and ARIC in southeastern Ohio are both housed in schools of medicine that have been well established as conveners of successful collaborative efforts. Ohio's schools and colleges of medicine have provided a validated and trusted third party with no ostensible institutional gain beyond further research into the practice and science of medicine. The knowledge resources of these institutions have been used to successfully accelerate the process of establishing and focusing local RHIO efforts.

The ongoing dialogue about health information technology and exchange that HPIO has supported now for the past three years has focused the attention of governmental, private and public hospitals, professional organizations and consumers on these topics. The Health Policy Institute of Ohio (HPIO), Wright State University Center for Healthy Communities (CHC) and Ohio KēPRO have co-sponsored state-wide Health Information Technology events in both 2004 and 2005, bringing together a variety of stakeholders to discuss HIT and HIE projects. On February 2006, HPIO and the Ohio Health Information Technology (OHHIT) Committee held a statewide meeting as a follow up to the 2005 Ohio HIT Summit to discuss the strategies that should be used to implement HIT and HIE across Ohio. In October 2006, the Third Annual OHHIT Summit was held and attended by 78 individuals representing the following stakeholder groups: physicians, behavioral health, consumers, pharmacy, state government, rural health, health plans, hospitals, long term care facilities and researchers.

Absent consistent standards for electronic reporting of quality measures from hospitals, the Ohio Hospital Association has established a process of collecting data from most hospitals around the state, centralizing and providing a kind of standardization of data reporting for the purpose of performance and quality review. The data arrives in non-standard form, is standardized, de-identified and shared with hospitals for their own quality review processes. Several regional hospital based quality initiatives have effectively established regional inter-organizational reviews that have resulted in improved practices. This process sets an important precedent for HIE for the purpose of quality measures.

The Ohio Hospital Association in conjunction with HPIO and HTP Inc. has provided education on health information exchange. At its annual meeting last year OHA hosted representatives from the Utah Health Information Network who provided a presentation on their project with the hope that Ohio could organize a network as a starting point for health information exchange using the technology tools and lessons learned from Utah.

The Ohio State Medical Association, the Ohio Association of Family Practice Physicians and the Ohio Osteopathic Association have provided a strong physician voice in all of the statewide discussion of HIT and HIE.

The State Office of Information Technology has organized a Sensitive Data Protection Working Group with representatives from twenty-eight state agencies. Through an administrative rule promulgated under sections 1306 and 1347 of the Ohio Revised Code, the Office of Information Technology is discussing setting baseline security standards specific to sensitive data so that agencies and universities account for risks associated with the sensitive data they hold and establish certain protections, if they are not already in place. The Sensitive Data Protection Working Group will recommend protections for sensitive data held by the state and develop an understanding of what potential impact such protections may have. It is anticipated that the group will meet two to three times to develop and vet their recommendations for inclusion in the proposed Ohio administrative rule.

- Identification of variations identified by the state and NOT being addressed by the proposed solutions presented in this report

None

4.0 Introduction to Analysis of Solutions

The Interim Analysis of Solutions Report has been revisited and augmented based on stakeholder review and Steering Committee discussion.

5.0 Review of State Solution Identification and Selection Process

- Discussion of the overall process used by the State to develop solutions

The SWG met primarily during the month of November. They began by discussing the primary findings of the Interim Assessment of Variations Report

(IAVR). Members were given the instruction that they were to review the IAVR and the HISPC wiki in preparation for discussion of the six points (barriers) identified in the executive summary of the IAVR. Members were asked to be prepared to make suggestions and offer solutions to listed barriers. Following each meeting, staff distributed minutes of these discussions and encouraged additional input between meetings. Staff then prepared an initial list of potential solutions generated during the meetings for review and comment. This initial list was also reviewed by the Steering Committee, who provided additional input. Following this, a draft of the Interim Solutions Report was circulated electronically to the SWG, followed by continued discussion both in meetings and electronically. The draft document was also posted on the wiki for broader review. All comments and additions were incorporated into the final draft for review by the SWG. At the last meeting of the SWG, members of the Implementation Working Group were also present, and they began to identify ways to implement the various solutions proposed. Concurrently, the final draft of the Interim Solutions Report was reviewed by the Steering Committee for comment. This report was made available to stakeholders who attended the five regional meetings that were held across Ohio during the months of December and January for further review and comment.

- Description of the State Solutions Workgroup, its charge, membership and stakeholder representation

The State Solutions Working Group has been charged by the Steering Committee with identifying potential solutions to the barriers specified in the IAVR. The SWG has 43 members and has representation from the following stakeholder groups: Attorneys, Behavioral health, Behavioral health IT, Community health centers, Consumers, Disease management vendors, Government IT, Home health care, Hospitals, Hospital association, Hospital IT, Long Term Care, Medicaid, Medical associations, Payers, Pharmacy, Physicians, Physician associations, Public health, Rural Public health, RHIOs, University, and Vendors.

- Description of the process used by the state to identify and propose solutions

The VWG report has set the universe of discussion for the barriers identified through that process. The SWG has reviewed those barriers and has suggested solutions that will be broadly reviewed by the LWG, VWG and stakeholders groups including clinicians, physician groups, health facilities and hospitals, payers, public health agencies, government health agencies, pharmacies, long-term care facilities and nursing homes, and consumers. The primary mechanism for feedback is the HISPC wiki.

- Description of the process used by the state to vet, evaluate and prioritize solutions

The Interim Solutions Report was broadly distributed to solicit input from all interested parties and as the Implementation Planning Working Group sought to

validate (vet) and to prioritize solutions. Potential implementations for solutions, included feasibility assessments, cost considerations and complications created by the solutions for specific groups like rural health care and health uninsured.

- Description of how solutions are organized and presented

Solutions are organized by barrier number.

- Description on how state has determined the level of feasibility of identified solutions

The Implementation Planning Working Group determined feasibility based on stakeholder discussions.

6.0 Analysis of State Proposed Solutions

6.1 Solutions to variations in organization business practices and policies

- Governance-related solutions
- Business arrangement solutions
- Technical solutions
- Guidance/Education solutions that address misinterpretation issues
- business agreements, and uniform patient consent / authorization forms

1b. At the state level, there should be a monitoring body that routinely reviews interpretation, compliance and practice related to the national standards. Planned compliance timelines are needed for smaller institutions and practices.
4 a. States should take responsibility for developing the basic infrastructure to support health information exchange.
4b. Any publicly funded HIE or HIT projects must be standards based including compliance with the Continuity of Care Record (CCR) standard or other generally accepted standards.
6a. Consumer education is needed to articulate the perceived value of health information exchange against the perceived risk of privacy and security breaches in an electronic system.
6b. Increased human oversight, evaluation of data integrity and enforcement of security protections are all recommended.

6.2 Solutions to issues derived from state privacy and security laws/regulations

- Solutions that would require changes in existing state law/regulations, e.g., draft model legislation
- Solutions that would require new state laws/regulations
- Solutions that would address issues of non-compliance with state laws/regulations
- Education solutions to address misinterpretations of state laws/regulations

5 a. Current laws and practices that govern the paper release of treatment related information should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.
5 b. The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, or any future standards gaining similar acceptance should be used as the standard for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.

6.3 Solutions to issues driven by intersection between federal and state laws/regulations

- Solutions applicable to general privacy/security federal laws and regulations (e.g., HIPAA Privacy, HIPAA Security)
- Solutions applicable to state programs (e.g., Medicaid)
- Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security)
- Education solutions to address misinterpretations of federal laws/regulations

1a. Approved n*ational standards not State standards are the solution.*
1c. E*lectronic messaging, elements of the clinical record, and transactions are increasingly electronic, national standards at this level should be adopted.*
1d. As *national standards are implemented, they should be in compliance with the existing standards as defined by HIPAA.*
2a. *Identify and use a unique identifier for patient identification in the NHIN, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included.*
2b. *In the future, accurate identification of patients should be through the use of biometrics.*
3a. *Standards need to be developed for role based access as defined initially by HIPAA with regard to treatment, payment and operations, and further defined in terms of both covered and non-covered entities and people likely to have access to data.*
3b. *The EHR audit trail, documenting by time and date stamp and source all read and write access to PHI, currently required under HIPAA regulations should be reinforced and required under state regulations for all health information exchange*.
3c. *Standardization of the application of the medical need to know and minimum necessary concepts as currently articulated in state and federal law should include specificity for read and write access in the exchange of PHI.*
3d. *Automatic reporting of access to one's records should be an option for consumers, with a formal process identified. There should be a standard process for consumer review and/or correction of data to insure integrity of data.*

3e. Formulate a model for best practices in security standards that will include a review of all existing security standards. This model should include a data classification schema.
5a. *Current laws and practices that govern the paper release of treatment related information should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*
5b. *The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, or any future standards gaining similar acceptance should be used for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.*
5c. ERISA, *FERPA and HIPAA regulations should be integrated.*
5d. S*pecific language should be developed which identifies conditions under which RHIOs or other clearinghouse organizations are routinely designated as covered entities*

6.4 Solutions to Enable Interstate e-Health Information Exchanges
None

7.0 National-level Recommendations

The focus of this project is on the solutions that the states and stakeholders can implement *at the organization, local, or state level* to develop privacy policy and security standards that will enable HIE on a nationwide scale. However, it is recognized that states and stakeholders may have recommendations for the federal government that could be of value to states as they grapple with the development of privacy policy and security standards. Such recommendations should be recorded in this section, and may include requests for guidance from the Office of Civil Rights on HIPAA Privacy and Security requirements. Any recommendation in this section should provide detailed examples of the issues and why federal involvement is the only recourse.

National standards are pivotal to the effective exchange of health information across organizations, states and territories. The states' responsibilities in health information exchange hinge upon the development and implementation of those standards. The recommendation that Ohio puts forward is to require the use of the Continuity of Care Record standard as the first adoption target. Multiple federal laws including FERPA, HIPAA, mental health and substance abuse law must be harmonized and guidance must be issued about the status of RHIOs as covered entities. Each state cannot provide solutions to these national issues, nor should they be asked to as such solutions might result in 50 or more variants, one from each state or territory.

8. Conclusions and Next Steps

To facilitate effective exchange of health information that will result in improved quality in health care, Ohio has engaged stakeholders in discussions to identify privacy and security barriers to health information exchange (HIE), potential

solutions, best practices, and specific plans to implement these solutions. To date, the results of these discussions have been summarized and are presented in the *Interim Assessment of Variations Report* and the *Interim Analysis of Solutions Report*. The purpose of this report is to articulate plans to implement those solutions within the context of Ohio's political, economic, social and legal environments.

Ohio is determined to maintain the momentum created by the OHHIT and HISPC initiatives through collaboration with the state governor's office. To date HPIO has met with representatives from both the state government and private sector to build on-going support, both financially and administratively for the next phase of implementation. To that end, the governor's office is currently reviewing an executive order that would continue the role of the HISPC Steering Committee as an interim step toward creating the proposed quasi-governmental organization. To further the value of participating in this collaborative effort, HPIO is also developing a strategic business plan that articulates the benefits of electronic health information exchange to all participants.